REMARKS

The claims remaining in the present application are Claims 1-20. The Examiner is thanked for performing a thorough search. None of the claims have been amended.

CLAIM REJECTIONS

35 U.S.C. §102

Claims 1-20

Claims 1-20 are rejected under 35 U.S.C. §102 as being anticipated by U.S. Patent No. 6,568,147 by Shanklin et al. (referred to hereinafter as "Shanklin"). Applicants respectfully submit that embodiments of the present invention are neither taught nor suggested by Shanklin.

The Office Action failed to specify which type of 102 was being used to reject Claims 1-20. Applicants respectfully request that the next Office Action completely specify the type of rejection that is being used.

Independent Claim 1 recites,

> A method of managing utilization of network intrusion detection systems in a dynamic data center, said method comprising:
>
> providing a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center;
>
> receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems; and
>
> automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy. (emphasis added)

Applicants respectfully submit that Shanklin does not teach or suggest, among other things, "said network intrusion detection systems in said dynamic data center ...receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems; and automatically

arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy," as recited by Claim 1

Referring to Shanklin's title and abstract, among other places, Shanklin teaches parallel intrusion detection sensors with load balancing for high speed networks where multiple sensors are connected at an internetworking device, which can be a router or a switch. The Office Action asserts that Shanklin teaches the embodiment recited by Claim 1 at Col. 1 line 63 through Col. 2 line 8. Col. 1 line 63 through Col. 2 line 8 states,

> One aspect of the invention is a method of detecting unauthorized access on a network as indicated by signature analysis of packet traffic on the network. A plurality of intrusion detection sensors are connected at a network entry point associated with an internetworking device, such as a router or switch. The packet load to the sensors is "load balanced", such that said packets are distributed at least at a session-based level. The load balancing may be at a lower (packet-based) level, which tends to more evenly distribute the load on each sensor but requires additional processing external to the sensors or requires sharing of session-level data between sensors. (emphasis added)

There is nothing in Shanklin about a dynamic data center and therefore Shanklin cannot teach "said network intrusion detection systems in said dynamic data center," as recited by Claim 1. Further, there is nothing in Shanklin about a monitoring policy therefore Shanklin cannot teach "receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems" nor can Shanklin teach "automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy."

It is not clear to Applicants what in Shanklin the Office Action asserts teaches "a plurality of monitoring points." For the sake of argument, Applicants shall assume that the Office Action intended to assert that Shanklin's "network entry points" are analogous to Claim 1's "plurality of monitoring points" (this is not an admission on the part of Applicants). However, note that Shanklin does not teach receiving Shanklin's network entry points. Further, Shanklin does not teach automatically arranging the monitoring of Shanklin's network entry points let alone teach

automatically arranging the monitoring of Shanklin's network entry points using network intrusion detection systems and a monitoring policy. Lastly, Shanklin does not teach that Shanklin's network entry points can be monitored with any network intrusion detection system.

For at least the forgoing reasons, Claim 1 should be patentable over Shanklin. Independent Claims 8 and 15 should be patentable for similar reasons that Claim 1 should be patentable.

Claims 2-7 depend on Claim 1. Claims 9-14 depend on Claim 8. Claims 16-20 depend on Claim 15. Therefore, these dependent claims should be patentable for at least the reasons that their respective independent claims should be patentable. Further, these dependent claims include additional limitations which further make them patentable. For example, Claims 2, 3, 4 further limit "said automatically arranging the monitoring of said monitoring points" and Claim 6 further limits "said receiving a monitoring policy and a plurality of monitoring points to be monitored."

CONCLUSION

In light of the above listed amendments and remarks, reconsideration of the rejected claims is requested. Based on the arguments presented above, it is respectfully submitted that Claims 1-20 overcome the rejections of record. For reasons discussed herein, Applicants respectfully request that Claims 1-20 be considered be the Examiner. Therefore, allowance of Claims 1-20 is respectfully solicited.

Should the Examiner have a question regarding the response, the Applicants invite the Examiner to contact the Applicants' undersigned representative at the below listed telephone number.

Respectfully submitted,
WAGNER BLECHER LLP

Dated: 4/11, 2007

John P. Wagner Jr.
Registration No. 35,398

Address: Westridge Business Park
123 Westridge Drive
Watsonville, California 95076 USA

Telephone: (408) 938-9060 Voice
(408) 234-3649 Direct/Cell
(408) 722-2350 Facsimile